PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-134189
(43)Date of publication of application : 21.05.1999

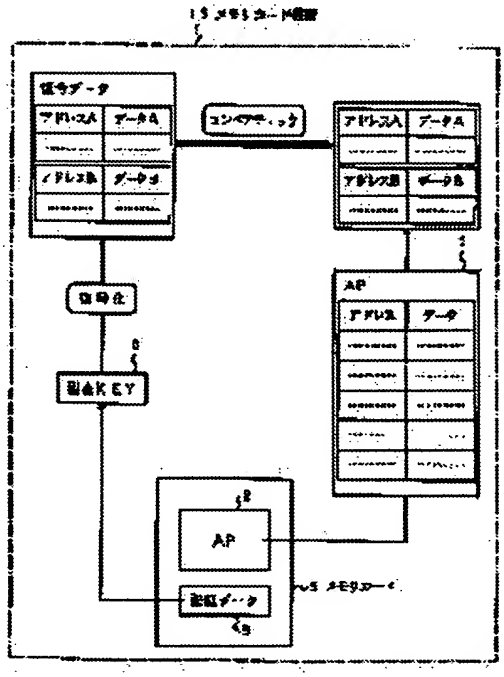
(51)Int.Cl. G06F 9/06
G06F 12/14
G06K 19/10

(21)Application number : 09-298446
(22)Date of filing : 30.10.1997

(71)Applicant : OKI ELECTRIC IND CO LTD
(72)Inventor : HARADA SEIICHI

(54) MEMORY CARD, AUTHENTICATION DATA GENERATION DEVICE AND MEMORY CARD DEVICE

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a memory card device checking the tuck or false of a memory card before an application program is executed and to provide a authentication data generation device for generation authentication data used for checking the truth or false and storing it in the memory card.
SOLUTION: Authentication data 9 obtained by ciphering an address which is read from the application program 2 at random and data stored in the address by a secret key 8 is stored in the memory card 5. Authentication data 9 is read from the memory card 5 and it is decoded by the secret key 8. Data which is read from the application program 2 based on the decoded address is compared with decoded data and the truth of false of the memory card 5 is checked.



LEGAL STATUS

[Date of request for examination] 29.02.2000
[Date of sending the examiner's decision of rejection] 21.10.2003
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection] 2003-22503
[Date of requesting appeal against examiner's decision of rejection] 20.11.2003

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平11－134189

(43)公開日　平成11年(1999)５月21日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｆ　9/06	５５０	Ｇ０６Ｆ　9/06	５５０Ｂ
			５５０Ｇ
12/14	３２０	12/14	３２０Ｂ
Ｇ０６Ｋ　19/10		Ｇ０６Ｋ　19/00	Ｒ

審査請求　未請求　請求項の数10　ＯＬ　（全 13 頁）

(21)出願番号　特願平9－298446

(22)出願日　平成９年(1997)10月30日

(71)出願人　000000295
沖電気工業株式会社
東京都港区虎ノ門１丁目７番12号

(72)発明者　原田　聖一
東京都港区虎ノ門１丁目７番12号　沖電気工業株式会社内

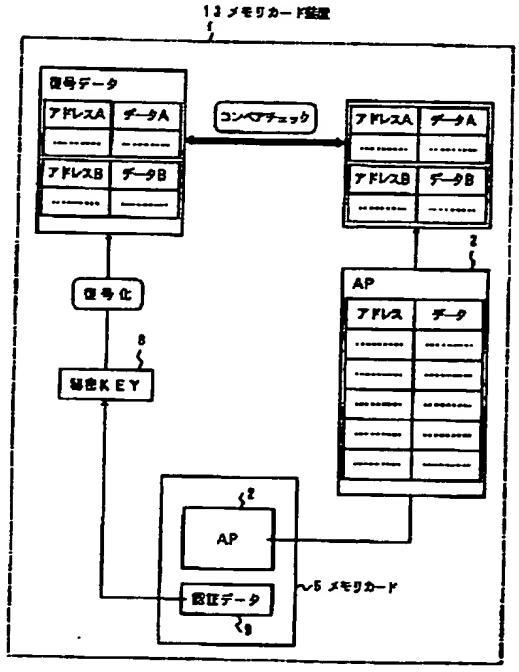
(74)代理人　弁理士　大西　健治

(54)【発明の名称】　メモリカードと認証データ作成装置とメモリカード装置

(57)【要約】

【課題】　アプリケーションプログラムを実行する前にメモリカードの真偽をチェックできるメモリカード装置と、その真偽のチェックに用いる認証データを作成してメモリカードに格納する認証データ作成装置とを提供する。

【解決手段】　アプリケーションプログラム２からランダムに読み出されたアドレスとそのアドレスに格納されたデータとを秘密キー８により暗号化した認証データ９をメモリカード５に格納し、メモリカード５から認証データ９を読み出して秘密キー８により復号化し、復号化されたアドレスに基づきアプリケーションプログラム２から読み出したデータと復号化されたデータとを比較してメモリカード５の真偽をチェックする。



メモリカード認証動作の説明図(1)

【特許請求の範囲】
【請求項１】　メモリカード装置に実装されるアプリケーションプログラムを格納したメモリカードにおいて、メモリカードの真偽チェックに用いる暗号化された認証データを格納していることを特徴としたメモリカード。
【請求項２】　請求項１に記載したメモリカードの認証データを作成する認証データ作成装置であって、
上記アプリケーションプログラムからランダムに読み出されたアドレスと該アドレスに格納されたデータとを秘密キーにより暗号化した認証データを上記メモリカードに格納することを特徴とした認証データ作成装置。
【請求項３】　上記秘密キーは、ランダムに読み出された上記アドレスを認証アドレスに暗号化するとともに該アドレスに格納されたデータを認証ハッシュ値に変換する請求項２記載の認証データ作成装置。
【請求項４】　メモリカードに格納されるアプリケーションプログラムからランダムに読み出されたアドレスと該アドレスに格納されたデータとを秘密キーにより暗号化した認証データを格納したメモリカードを実装するメモリカード装置であって、
上記メモリカードから認証データを読み出して上記秘密キーにより復号化し、復号化されたアドレスに基づき上記アプリケーションプログラムから読み出したデータと復号化されたデータとを比較してメモリカードの真偽をチェックすることを特徴とするメモリカード装置。
【請求項５】　上記認証データは、ランダムに読み出された上記アドレスを上記秘密キーにより暗号化した認証アドレスと、該アドレスに格納されたデータを上記秘密キーにより変換した認証ハッシュ値とからなり、認証アドレスを上記秘密キーにより復号化するとともに復号化されたアドレスに基づき上記アプリケーションプログラムから読み出されたデータを比較ハッシュ値に変換し、該比較ハッシュ値と上記認証ハッシュ値とを比較してメモリカードの真偽をチェックする請求項４記載のメモリカード装置。
【請求項６】　リセットボタンの押下により上記メモリカードの真偽の認証処理を行い、該メモリカードが真の場合には装置のメモリに認証ＯＫフラグデータをセットし、以後、電源ボタン押下により上記認証ＯＫフラグデータのセット状態をチェックし、セットならば該メモリカードを真と認証する請求項４記載、又は請求項５記載のメモリカード装置。
【請求項７】　リセットボタンの押下により上記メモリカードの真偽の認証処理を行い、該メモリカードが真の場合には装置のメモリに認証ＯＫフラグデータをセットするとともにメモリカードの認証データをクリアし、以後、電源ボタン押下により上記認証ＯＫフラグデータのセット状態をチェックし、セットならば該メモリカードを真と認証する請求項４記載、又は請求項５記載のメモリカード装置。
【請求項８】　電源ボタンを押下する毎に上記メモリカードの真偽の認証処理を行う請求項４記載のメモリカード装置。
【請求項９】　待ち状態が予め決められた時間経過すると、装置を低消費電力モードに切り替える請求項４記載、又は請求項５記載のメモリカード装置。
【請求項１０】　上記メモリカードが装置から抜去された場合には装置のメモリにセットされた上記認証フラグをクリアする請求項４記載、又は請求項５記載のメモリカード装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は電子商取引に使用される携帯型電子機器等のメモリカードを使用するメモリカード装置と、そのメモリカードに格納する認証データを作成する認証データ作成装置とに関する。
【０００２】
【従来の技術】従来、メモリカード装置、例えば、電子商取引に使用される携帯型電子機器では、アプリケーションプログラムが格納されてあるメモリカードをメモリカード装置に挿入すると、アプリケーションプログラムが即、実行される。
【０００３】
【発明が解決しようとする課題】従来のメモリカード装置にあっては、メモリカードの真偽をチェックする機能が設けてないので、メモリカードがメモリカード装置に挿入されると、たとえ不正なアプリケーションプログラムが実装してあっても実行されてしまい、電子商取引の内容が書き替えられてしまう恐れがあるという問題点があった。
【０００４】本発明はアプリケーションプログラムを実行する前にメモリカードの真偽をチェックできるメモリカード装置と、その真偽のチェックに用いる認証データを作成してメモリカードに格納する認証データ作成装置とを提供することを目的としている。
【０００５】
【課題を解決するための手段】上記目的を達成するために本発明は、アプリケーションプログラムからランダムに読み出されたアドレスと該アドレスに格納されたデータとを秘密キーにより暗号化した認証データをメモリカードに格納する認証データ作成装置と、メモリカードから認証データを読み出して秘密キーにより復号化し、復号化されたアドレスに基づきアプリケーションプログラムから読み出したデータと復号化されたデータとを比較してメモリカードの真偽をチェックするメモリカード装置とを備える。
【０００６】
【発明の実施の形態】本発明の実施の形態について図面を参照しながら説明する。尚、各図面に共通な要素には同一符号を付す。

第１の実施の形態

図２はメモリカードライタの構成を示すブロック図である。メモリカードライタ１は、後述するメモリカード装置で実行されるアプリケーションプログラム２（以後ＡＰ２と記す）を格納した媒体３（以後ＡＰ媒体３と記す）を挿抜するＡＰ用Ｉ／Ｏスロット４と、メモリカード５を挿抜するメモリカード接続用Ｉ／Ｏスロット６と、書き込み開始スイッチ７とを有する。

【０００７】ＡＰ媒体３、メモリカード５はＡＰ用Ｉ／Ｏスロット４、メモリカード接続用Ｉ／Ｏスロット６に設けられた図示せぬコネクタに挿抜する端子部３ａ、５ａを有する。

【０００８】メモリカードライタ１には、ＡＰ２の実行コードから、例えば１ＫＢ（キロバイト）程度のアドレスとデータとのセットをランダムに選択し、そのセットデータを秘密キー８（以後秘密ＫＥＹ８と記す）を用いて暗号化し、認証データ９としてメモリカード５に格納する認証データ作成手段１０と、ＡＰ２をメモリカード５に書き込むＡＰ書き込み手段１１とを内蔵している。

【０００９】具体的には、図示せぬメモリに格納してある認証データ作成プログラム、ＡＰ書き込みプログラムをＣＰＵ１２が実行することによって各手段を達成する。

【００１０】アドレスとデータとのセットをランダムに選択するには、例えば、乱数を発生させ、その乱数でアドレスを構成してデータを選択するプログラムを認証データ作成プログラムに含ませておく。

【００１１】図３はメモリカード装置の外観斜視図、図４は図３に示したメモリカード装置に搭載される制御ブロック図である。メモリカード装置１３、例えば、電子商取引に使用される携帯型電子機器は、表面に操作キー群１４、表示部１５を備えてある。側面には矢印Ａ－Ｂ方向にメモリカード５を挿抜する際に用いるメモリカード挿入口１６及びメモリカード挿入口１６に挿入した際メモリカード５をロックする矢印Ｃ－Ｄ方向に移動自在なスライダ１７を有する。

【００１２】操作キー群１４には電源ボタン１４ａ、リセットボタン１４ｂ、テンキー等があり、表示部１５には操作に伴うメッセージが表示される。

【００１３】メモリカード装置１３の内部には、メモリカード挿入口１６から挿入されるメモリカード５と並行になるように、破線で示す基板１８が搭載してある。基板１８には、図４に示すように、中央処理装置１９（以後ＣＰＵ１９と記す）、ＲＯＭ２０、ＲＡＭ２１、バッテリー２２等が搭載されてある。バッテリー２２はＣＰＵ１９、ＲＯＭ２０、ＲＡＭ２１にライン２３を通じて電力を供給し、ＣＰＵ１９はＲＯＭ２０、ＲＡＭ２１とバスライン２４で接続されている。

【００１４】ＲＯＭ２０には制御プログラム２０ａ、認証プログラム２０ｂ、秘密キー８（以後秘密ＫＥＹ８と記す）が格納してあり、ＲＡＭ２１はメモリカード５から読み込まれたＡＰ２の格納や各種処理時のデータ格納に用いられる。秘密ＫＥＹ８はメモリカード５の認証データ９を復号化する際に用いられるもので外部からの読み出しに対しプロテクトされてある。

【００１５】ＣＰＵ１９は認証プログラム２０ｂを実行することによりメモリカード認証手段２６となり、メモリカード５が真の場合には表示部１５に「ＡＰの実行に移る」旨のメッセージを表示するとともに、ＲＡＭ２１にメモリカード５が真であることを示す認証ＯＫフラグデータ２１ａをセットする。

【００１６】また、ＣＰＵ１９は制御プログラム２０ａを実行することによりタイマ手段２５、低電力消費モード切替手段２７、カード実装チェック手段２８、カード引き抜きチェック手段２９等になる。

【００１７】低電力消費モード切替手段２７はタイマ手段２５を用い、待ち状態が予め決められた時間経過すると、ＣＰＵ１９をホールド状態に切り替え、無駄な電力消費を抑える。カード実装チェック手段２８はメモリカード５の端子部５ａが差し込まれるコネクタの状況を表すレジスタの内容をタイマ手段２５を用い、例えば１秒割り込みで確認する。

【００１８】また、スライダ１７を矢印Ｄ方向に移動させると、マスク不可能な割り込み信号（ＮＭＩ）がＣＰＵ１９に送られ、カード引き抜きチェック手段２９がＲＡＭ２１の認証ＯＫフラグデータ２１ａをクリアする。

【００１９】次に動作について説明する。先ず、図５を参照してメモリカードライタ１の動作について説明する。ＡＰ２を格納したＡＰ媒体３、何も書き込まれていないメモリカード５を、それぞれ、ＡＰ用Ｉ／Ｏスロット４、メモリカード接続用Ｉ／Ｏスロット６に挿入し、書き込み開始スイッチ７を押下する。

【００２０】ＣＰＵ１２はＡＰ書き込み手段１１としてＡＰ媒体３からＡＰ２を読み込み、メモリカード５に書き込む。

【００２１】次に、ＣＰＵ１２は認証データ作成手段１０としてＡＰ２からアドレスとデータとのセット２ａをランダムに選択し、そのセットデータ２ａを秘密ＫＥＹ８を用いて暗号化し、認証データ９としてメモリカード５に書き込む。

【００２２】次に、図１、図６を参照してメモリカード認証動作について説明する。図１は第１の実施の形態によるメモリカード認証動作の説明図（１）、図６は第１の実施の形態によるリセットボタン押下後の動作を示すフローチャート（１）である。メモリカード５の端子部５ａをメモリカード装置１３のメモリカード挿入口１６から矢印Ａ方向へ挿入する。端子部５ａはメモリカード装置１３の内部に設けられた図示せぬコネクタに差し込まれる。

【００２３】メモリカード５には、メモリカードライタ

１によりＡＰ２、認証データ９が格納されてある。リセットボタン１４ｂが押下されると、ステップS1 でＣＰＵ１９は制御プログラム２０ａに基づきメモリカード装置１３を初期化する。初期化によって、ＲＡＭ２１の認証ＯＫフラグデータ２１ａもクリアされる。

【００２４】ステップS2 でＣＰＵ１９はメモリカード認証手段２６として、図１に示すように、メモリカード５からＡＰ２を読み出し、ＲＡＭ２１に格納する。ステップS3 でメモリカード５から認証データ９を読み出し、秘密ＫＥＹ８を用いて復号化し、復号データとしてＲＡＭ２１に格納する。

【００２５】ステップS4 で復号データのアドレスに基づいてＲＡＭ２１に格納してあるＡＰ２からデータを読み出す。即ち、ＣＰＵ１９は復号データのアドレスを図示せぬプログラムカウンタに入力し、ＲＡＭ２１に格納してあるＡＰ２からデータを読み出す。

【００２６】ステップS5 でＡＰ２から読み出したデータと復号データのデータとを比較する。即ち、ＣＰＵ１９はＡＰ２から読み出したデータと復号データのデータとを図示せぬ演算部のレジスタにセットして比較する。ステップS6 で一致ならばステップS7 に分岐し、否ならばステップS9 に分岐する。

【００２７】ステップS7 で比較するデータが未だ有るか否かをチェックし、有ればステップS5 に分岐し、否ならばステップS8 に分岐する。ステップS8 でＣＰＵ１９は表示部１５に「ＡＰの実行に移る」旨のメッセージを表示するとともに、ＲＡＭ２１に認証ＯＫフラグデータ２１ａをセットし、メモリカード認証動作を終了する。

【００２８】ステップS9 でＣＰＵ１９は表示部１５に「メモリカードは不正である」旨のメッセージを表示してメモリカード認証動作を終了する。

【００２９】次に図７を参照して電源ボタン押下後の動作を説明する。図７は第１の実施の形態による電源ボタン押下後の動作を示すフローチャート（１）である。電源ボタン１４ａが押下されると、ステップS10でＣＰＵ１９はメモリカード認証手段２６として、ＲＡＭ２１の認証ＯＫフラグデータ２１ａがセットされているか否かをチェックし、セットされていればステップS11に分岐し、否ならばステップS12に分岐する。

【００３０】ステップS11でＣＰＵ１９は表示部１５に「ＡＰの実行に移る」旨のメッセージを表示し、メモリカード認証動作を終了する。ステップS12でＣＰＵ１９は表示部１５に「メモリカードは不正である」旨のメッセージを表示し、メモリカード認証動作を終了する。

【００３１】次に図８を参照してカード引き抜き後の動作を説明する。メモリカード認証動作は終了してＲＡＭ２１に認証ＯＫフラグデータ２１ａがセットされている。メモリカード５を引き抜くためにスライダ１７を矢印D方向に移動させると、ステップS20でＣＰＵ１９はカード引き抜きチェック手段２９としてマスク不可能な割り込み信号（ＮＭＩ）が発生したか否かをセンスしており、発生ならばステップS21に分岐する。ステップS21でＲＡＭ２１の認証ＯＫフラグデータ２１ａをクリアするとともに表示部１５に「認証ＯＫフラグデータをクリアした」旨のメッセージを表示して処理を終了する。従って、次回ＡＰを実行させるには、リセットボタン１４ｂを押下しなければならない。

【００３２】第１の実施の形態によれば、メモリカードライタを装置ベンダーから信頼できるユーザ（システムベンダー、ソフトハウス等）に提供、管理させることでユーザライタブルでしかも、セキュリティを持ったメモリカードの提供が可能なシステムを実現できる。

【００３３】また、ＡＰの実行コードのアドレスとデータとからなるセットデータを暗号化して認証データを作成してメモリカードに格納し、メモリカード装置で認証データを復号化し、ＡＰと比較してメモリカードの真偽をチェックできるようにしたので、不正なＡＰが実行される恐れはなくなる。

【００３４】また、メモリカード装置にＡＰに関する情報が実装されていなくともメモリカードの真偽がチェックできるので、ＡＰのバージョンアップ等の変更が生じても、メモリカード装置側では何の変更も伴わず、変更後のメモリカードの真偽をチェックできる。

【００３５】また、リセットボタン押下に伴うメモリカードの真偽チェックで真と判定されれば、以後、電源ボタン押下に伴う認証ＯＫフラグデータのチェックでメモリカードの真偽チェックを行えるので、真偽チェックに要する時間を短縮できる。

【００３６】また、メモリカード装置からメモリカードが引き抜かれた場合、認証ＯＫフラグデータをクリアするようにしたことにより、その後、偽造メモリカードをメモリカード装置に実装し、電源ボタンを押下しても「メモリカードは不正である」旨のメッセージを表示されるので、偽造メモリカードの使用を防止できる。

【００３７】第２の実施の形態

第２の実施の形態が第１の実施の形態と異なるところは、電源ボタンがリセットボタンをも兼ねている点と、メモリカード認証手段がＲＡＭ２１に認証ＯＫフラグデータ２１ａをセットしない点である。

【００３８】図９は第２の実施の形態によるフローチャートである。第１の実施の形態のメモリカード認証動作と異なるところは、電源ボタン１４ａが押下される毎に、ＣＰＵ１９はリセットされ、ステップS1 でメモリカード装置１３を初期化する点と、ステップS8 でＲＡＭ２１に認証ＯＫフラグデータ２１ａをセットしない点である。

【００３９】第２の実施の形態によれば、メモリカード装置を立ち上げる（電源ボタンを押下する）毎に、ＣＰＵはメモリカードの認証動作を行うので、第１の実施の

形態による認証ＯＫフラグデータセットに比べてセキュリティが向上し、不正なアプリケーションプログラムが実行される恐れはなくなる。

【００４０】第３の実施の形態

第３の実施の形態が第１の実施の形態と異なるところは、リセットボタン押下により開始されるメモリカードの認証動作である。即ち、認証動作によりメモリカードが真であれば、ＲＡＭ２１に認証ＯＫフラグデータ２１ａをセットするとともに、メモリカード２の認証データをクリア（例えば認証データに有効ビット、無効ビットを立てるようにしておきメモリカードが真であれば無効ビットを立てる）にする点である。

【００４１】動作については第１の実施の形態と同じであるから省略する。

【００４２】第３の実施の形態によれば、ＡＰ認証後、メモリカードの認証データをクリアすることにより、一度認証されたメモリカード（又は、その不正コピー）を他のメモリカード装置で再利用することを不可能にし、さらに、メモリカード装置に実装されて出荷されたメモリカードからの読み出しを不可能にし、偽造メモリカードの製造を防止させることができる。

【００４３】第４の実施の形態

第４の実施の形態が第１の実施の形態と異なるところは、メモリカードライタ１により認証データ９を作成する際、秘密ＫＥＹを用いてアドレスを認証アドレスに暗号化するとともにデータを認証ハッシュ値に変換する。

【００４４】メモリカード装置１３では、秘密ＫＥＹを用いて認証アドレスを復号化し、復号化されたアドレスに基づいてＡＰからデータを読み出し、秘密ＫＥＹを用いてデータから比較ハッシュ値を求め、認証ハッシュ値と比較してメモリカードの真偽をチェックする。

【００４５】図１０は第４の実施の形態によるメモリカードライタの動作を示す説明図である。先ず、図２に示したように、ＡＰ２を格納したＡＰ媒体３、何も書き込まれていないメモリカード５を、それぞれ、ＡＰ用Ｉ／Ｏスロット４、メモリカード接続用Ｉ／Ｏスロット６に挿入し、書き込み開始スイッチ７を押下する。

【００４６】ＣＰＵ１２はＡＰ書き込み手段１１として、図１０に示すように、ＡＰ媒体３からＡＰ２を読み込み、メモリカード５に書き込む。

【００４７】次に、ＣＰＵ１２は認証データ作成手段１０として、読み込んだＡＰ２からアドレスとデータとのセットデータ２ａをランダムに選択し、そのセットデータ２ａと秘密ＫＥＹ３０とを用いて認証データ９を作成し、メモリカード５に書き込む。

【００４８】セットデータ２ａのうち、アドレスは秘密ＫＥＹ３０を用いて暗号化され、認証アドレス９ａとしてメモリカード５に書き込まれる。同様に、データは秘密ＫＥＹ３０を用いてハッシュ値に変換され、認証ハッシュ値９ｂとしてメモリカード５に書き込まれる。

【００４９】図１１は第４の実施の形態によるメモリカード認証動作の説明図、図１２は第４の実施の形態によるリセットボタン押下後の動作を示すフローチャート（２）である。

【００５０】メモリカード５には、メモリカードライタ１によりＡＰ２、認証データ９が格納されてある。リセットボタン１４ｂが押下されると、ステップS1 でＣＰＵ１９は制御プログラム２０ａに基づきメモリカード装置１３を初期化する。初期化によって、ＲＡＭ２１の認証ＯＫフラグデータ２１ａもクリアされる。

【００５１】ステップS2 でＣＰＵ１９はメモリカード認証手段２６として、図１１に示すように、メモリカード５からＡＰ２を読み出し、ＲＡＭ２１に格納する。ステップS3 でメモリカード５から認証アドレス９ａを読み出し、秘密ＫＥＹ３０を用いて復号化し、復号アドレス３１としてＲＡＭ２１に格納する。

【００５２】ステップS4 で復号アドレス３１に基づいてＲＡＭ２１に格納してあるＡＰ２からデータを読み出し、データ群３２としてＲＡＭ２１に格納する。即ち、ＣＰＵ１９は復号化されたアドレスを順に図示せぬプログラムカウンタに入力し、ＲＡＭ２１に格納してあるＡＰ２からデータを読み出す。

【００５３】ステップS5 で秘密ＫＥＹ３０を用いてデータ群３２からハッシュ値を算出し、比較ハッシュ値３３としてＲＡＭ２１に格納する。ステップS6 でメモリカード５の認証ハッシュ値９ｂと比較ハッシュ値３３とを比較する。即ち、ＣＰＵ１９は認証ハッシュ値９ｂと比較ハッシュ値３３とをＲＡＭ２１から図示せぬ演算部のレジスタにセットして比較する。ステップS7 で一致ならばステップS8 に分岐し、否ならばステップS10に分岐する。

【００５４】ステップS8 でＣＰＵ１９は表示部１５に「ＡＰの実行に移る」旨のメッセージを表示するとともに、ＲＡＭ２１に認証ＯＫフラグデータ２１ａをセットし、メモリカード認証動作を終了する。

【００５５】ステップS9 でＣＰＵ１９は表示部１５に「メモリカードは不正である」旨のメッセージを表示してメモリカード認証動作を終了する。

【００５６】第４の実施の形態によれば、データは最後のハッシュ値を認証ハッシュ値としてメモリカードに格納されるようにしたので、第１の実施の形態に比べてメモリカードに実装する認証データのサイズを大幅に小さくすることができる。

【００５７】

【発明の効果】本発明は、以上説明したように構成されているので以下に記載される効果を奏する。アプリケーションプログラムと暗号化した認証データとを格納したメモリカードをメモリカード装置に実装し、認証データを復号化して得られたアドレスによりアプリケーションプログラムから読み出したデータ、あるいは読み出して

処理したデータと、認証データから得られたデータと比較してメモリカードの真偽をチェックするようにしたことにより、不正なアプリケーションプログラムを実装したメモリカードがメモリカード装置に挿入されても実行されないので、電子商取引の内容等が書き替えられてしまう恐れがなくなる。

【図面の簡単な説明】

【図１】メモリカード認証動作の説明図（１）である。

【図２】メモリカードライタの構成を示すブロック図である。

【図３】メモリカード装置の外観斜視図である。

【図４】メモリカード装置に搭載される制御ブロック図である。

【図５】メモリカードライタの動作を示す説明図（１）である。

【図６】リセットボタン押下後の動作を示すフローチャート（１）である。

【図７】電源ボタン押下後の動作を示すフローチャート（１）である。

【図８】カード引き抜き後の動作を示すフローチャートである。

【図９】電源ボタン押下後の動作を示すフローチャート（２）である。

【図１０】メモリカードライタの動作を示す説明図（２）である。

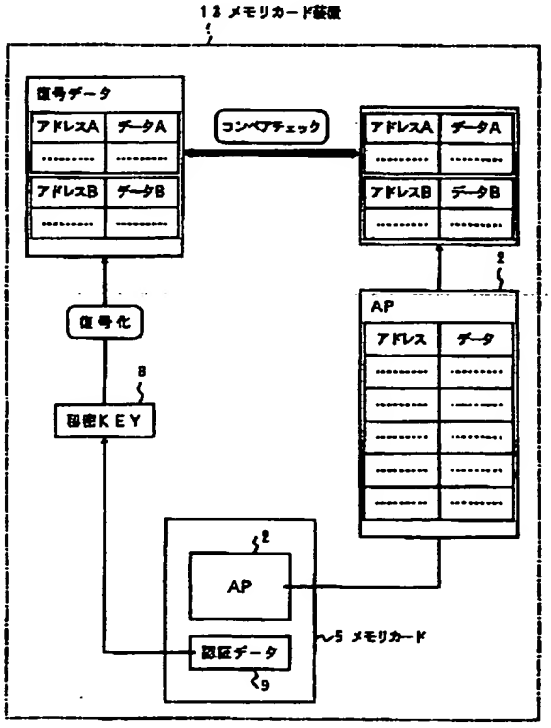
【図１１】メモリカード認証動作の説明図（２）である。

【図１２】リセットボタン押下後の動作を示すフローチャート（２）である。

【符号の説明】

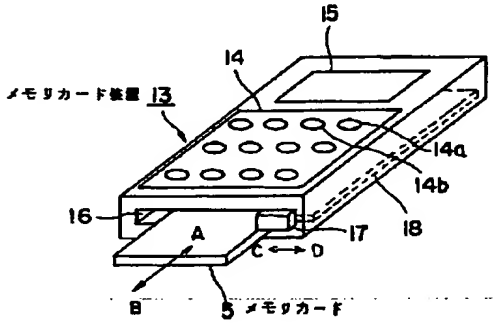
１　メモリカードライタ
３　ＡＰ媒体
５　メモリカード
８、３０　秘密ＫＥＹ
１２、１９　ＣＰＵ
１３　メモリカード装置
２０　ＲＯＭ
２１　ＲＡＭ

【図１】



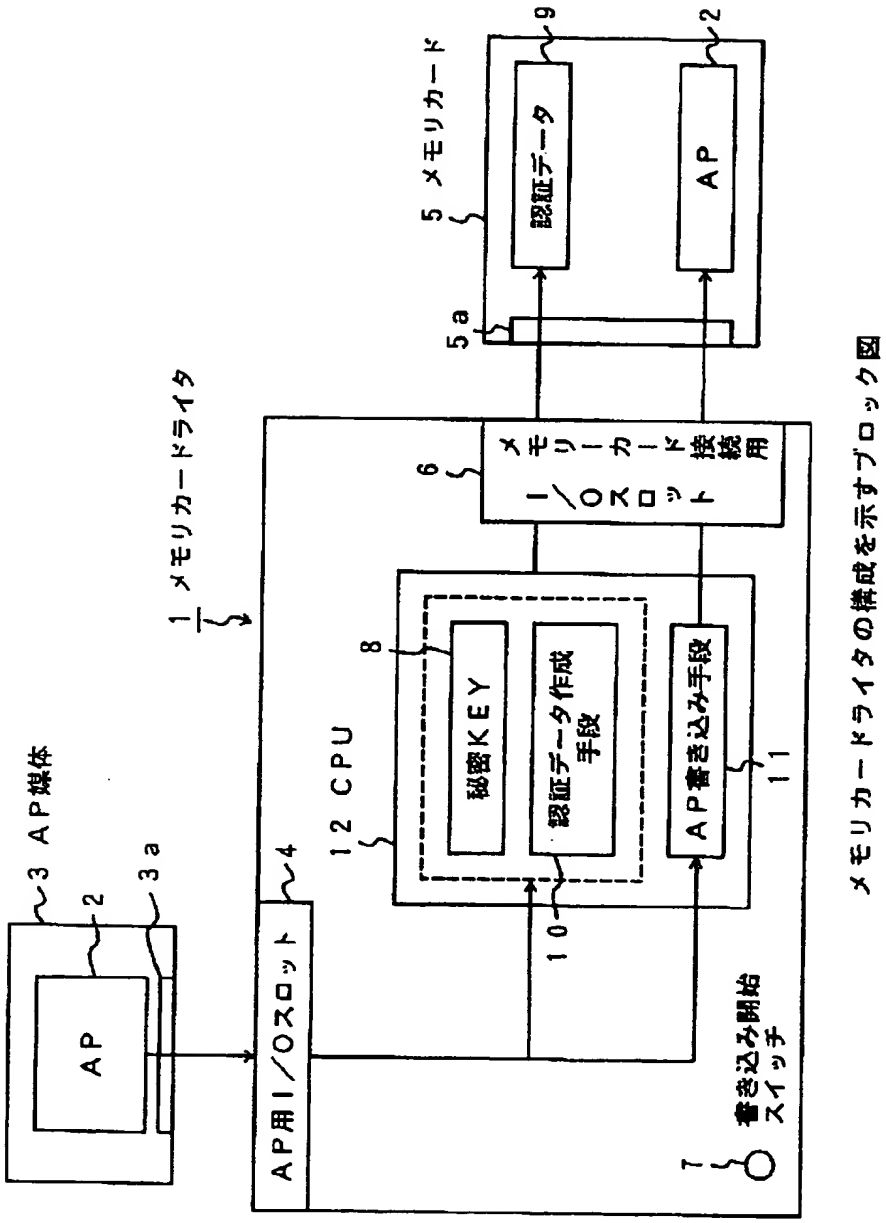
メモリカード認証動作の説明図(1)

【図３】



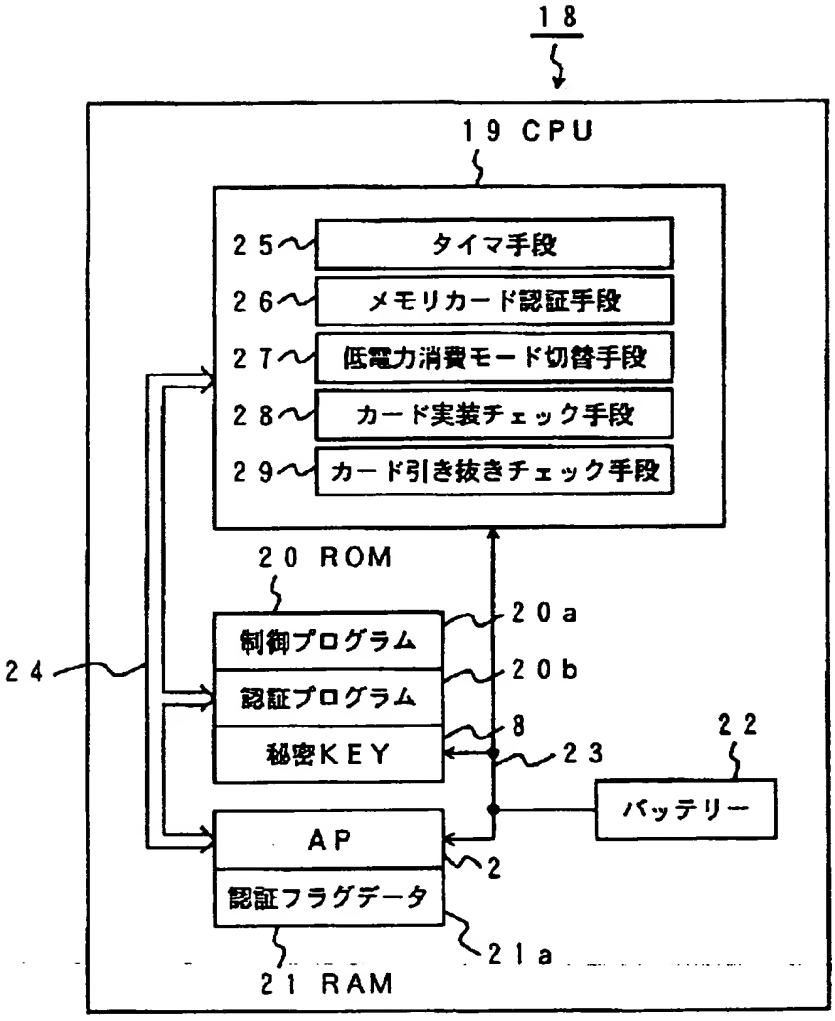
メモリカード装置の外観斜視図

【図2】



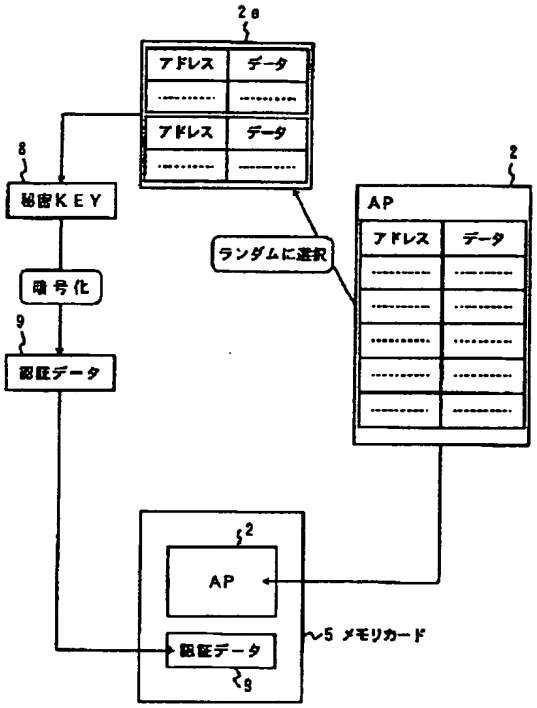
メモリカードライタの構成を示すブロック図

【図４】



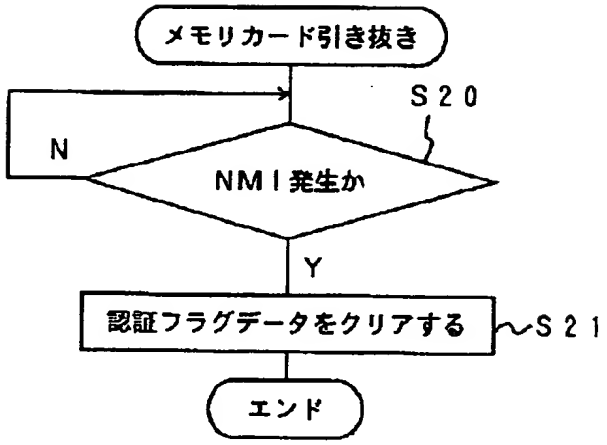
メモリカード装置に搭載される制御ブロック図

【図５】



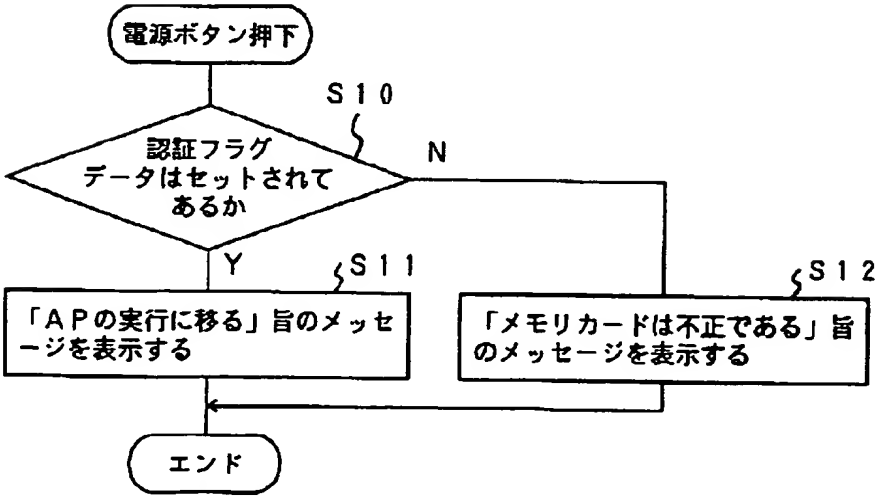
メモリカードライタの動作を示す説明図

【図８】



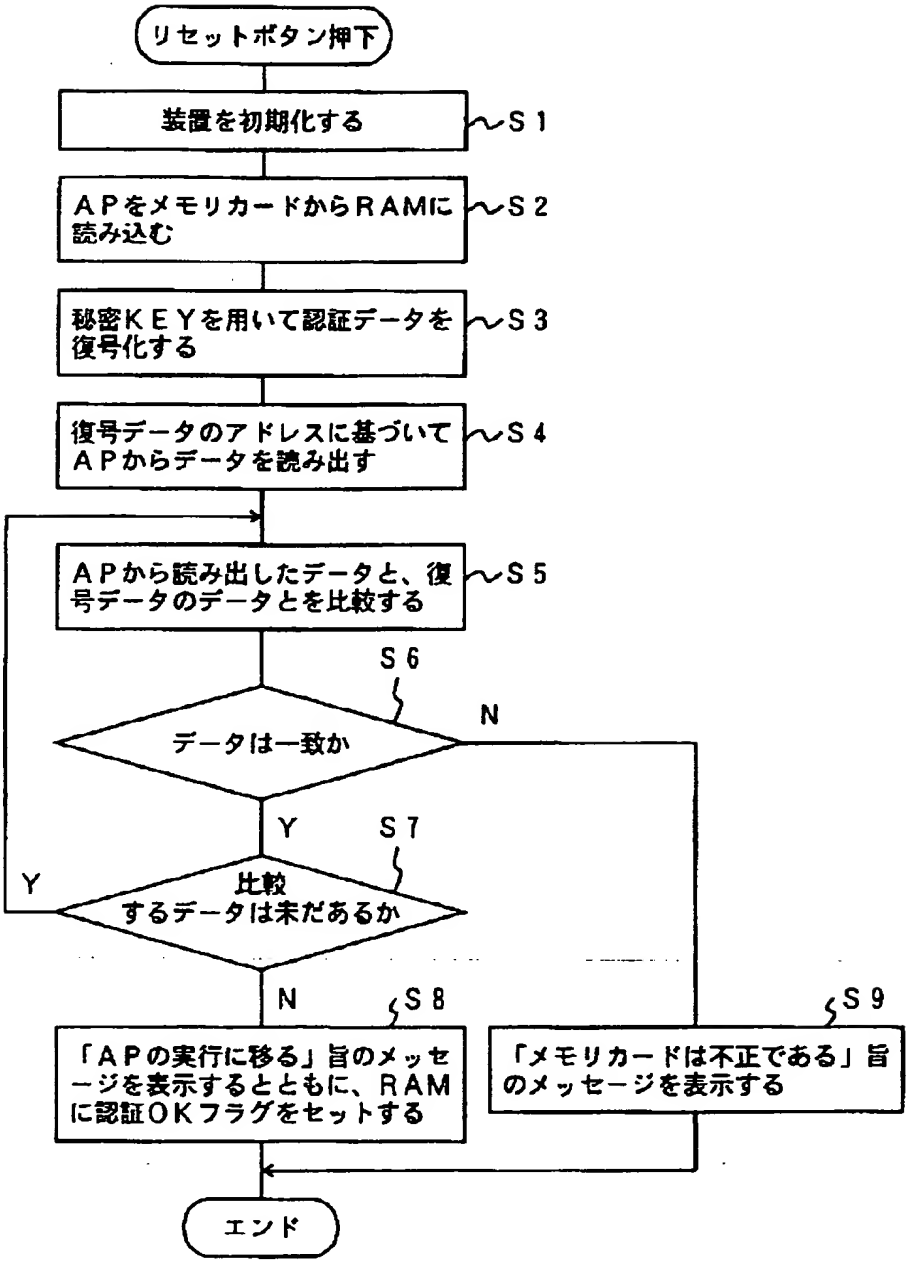
カード引き抜き後の動作を示すフローチャート

【図７】



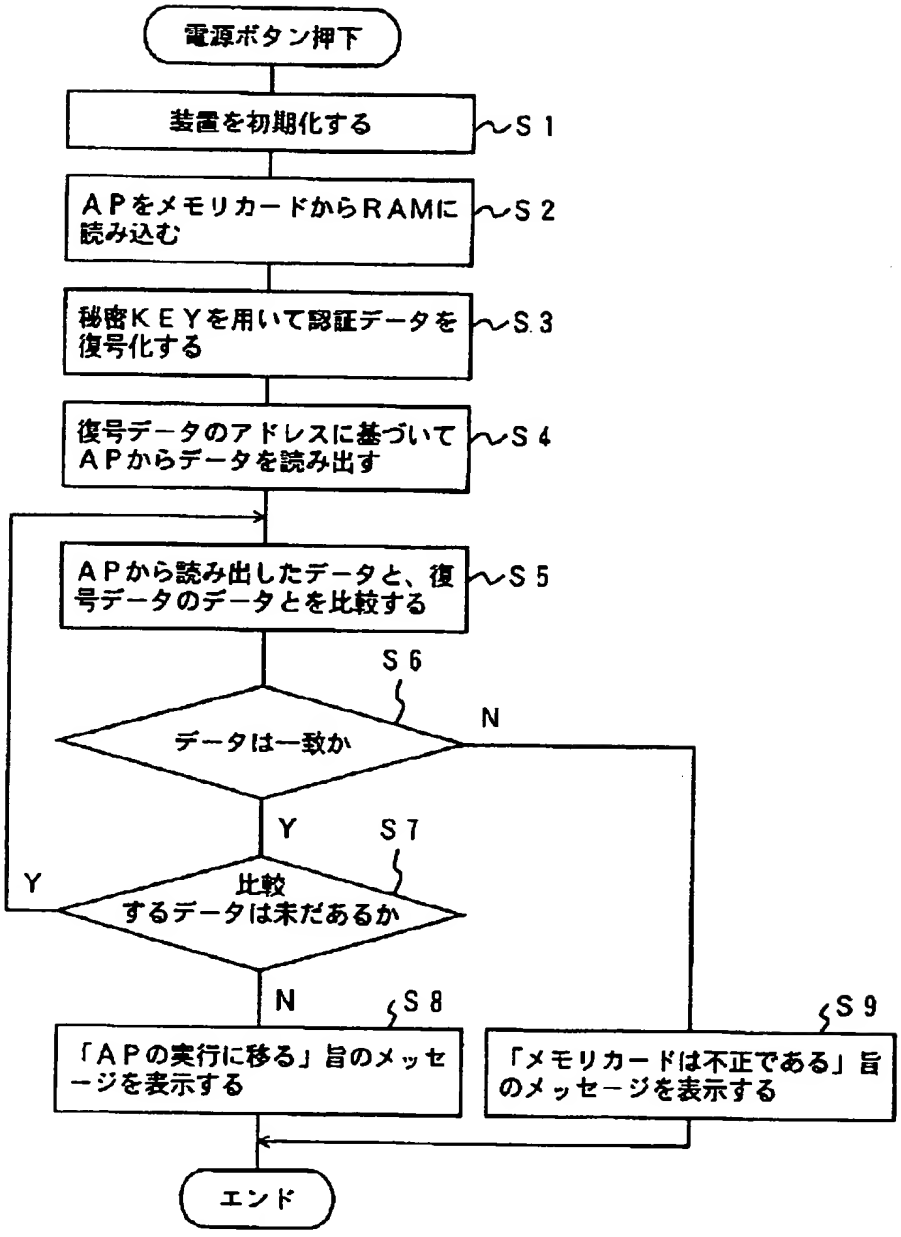
電源ボタン押下後の動作を示すフローチャート

【図６】



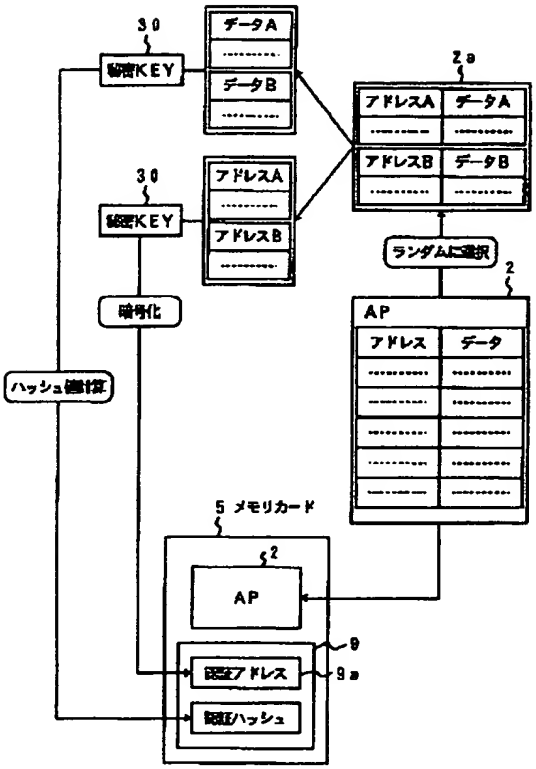
リセットボタン押下後の動作を示すフローチャート(1)

【図９】



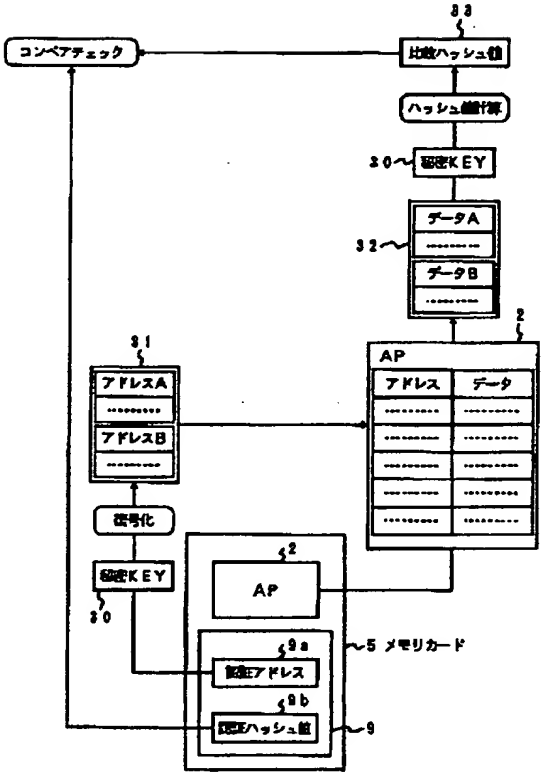
リセットボタン押下後の動作を示すフローチャート(2)

【図１０】



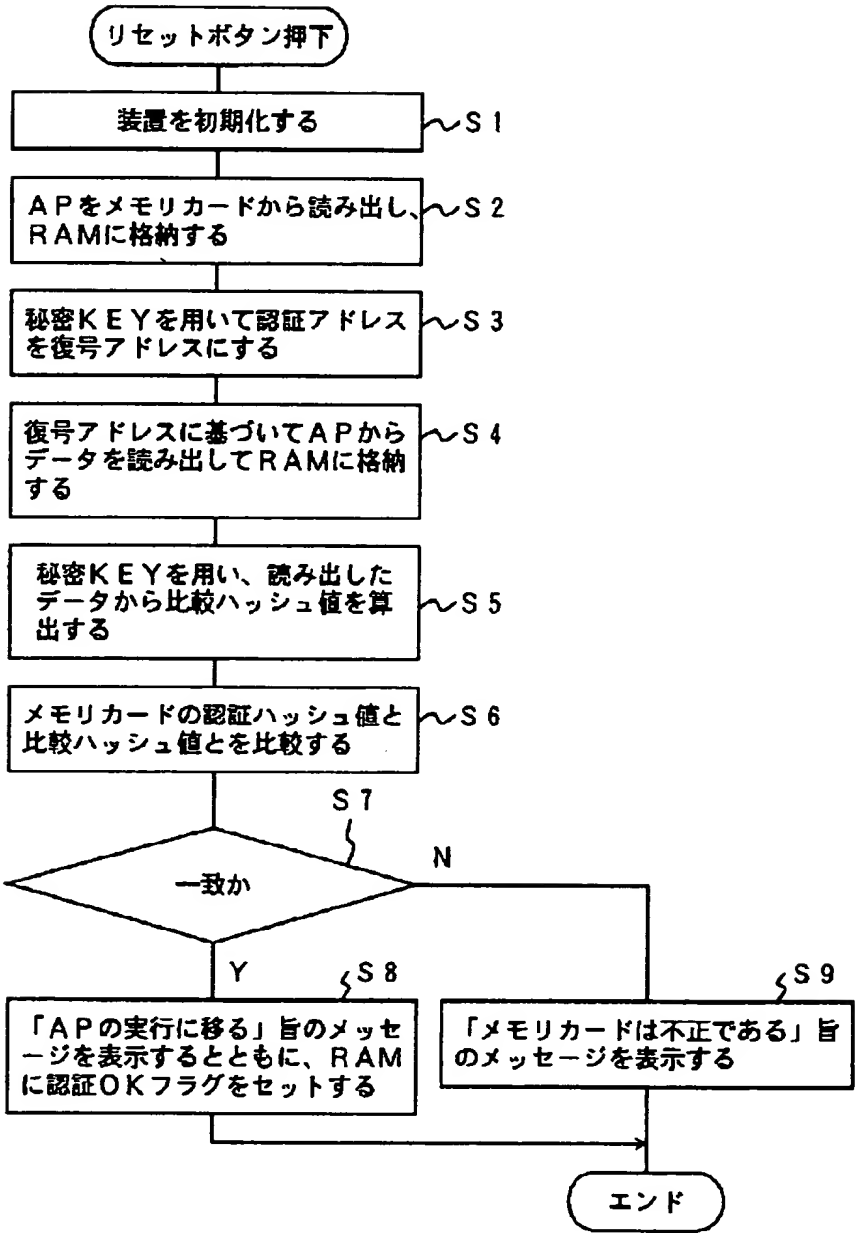
メモリカードライタの動作を示す説明図(2)

【図１１】



メモリカード認証動作の説明図(2)

【図１２】



リセットボタン押下後の動作を示すフローチャート(3)